⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　昭63-244288

⑤Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和63年(1988)10月11日
G 06 K 17/00		T-6711-5B	
G 06 F 15/21	340	B-7230-5B	

審査請求　未請求　発明の数 1　(全4頁)

⑤発明の名称　ICカード暗証照合システム

⑳特　願　昭62-77726
㉒出　願　昭62(1987)3月31日

㉑発明者　伊藤　守　大阪府門真市大字門真1006番地　松下電器産業株式会社内
㉑出願人　松下電器産業株式会社　大阪府門真市大字門真1006番地
㉔代理人　弁理士　中尾　敏男　外1名

明　細　書

1、発明の名称

ICカード暗証照合システム

2、特許請求の範囲

(1) カード所持者が暗証符号を入力する暗証符号入力手段、前記暗証符号入力手段から得られる第1の入力暗証符号を用いて暗号化鍵を生成する暗号化鍵生成手段、および前記暗号化鍵を用いて前記第1の入力暗証符号を暗号化された第2の入力暗証符号に変換する暗証符号暗号化手段を具備する暗証入力装置と、カード発行時などに登録される登録暗証符号を記憶するメモリ手段、および前記登録暗証符号と前記第2の入力暗証符号との照合を行い照合結果を出力する暗証照合手段を具備するICカードと、前記暗証入力装置から得られる第2の入力暗証符号を前記ICカードに書き込み、前記ICカードから前記登録暗証符号と前記第2の入力暗証符号の照合結果を読み出すICカード端末機とを有し、前記登録暗証符号を、前記暗号化鍵と同一の暗号化鍵と前記暗証符号暗号化手段と同一の手続きを用いて暗号化し、前記メモリ手段にそえもって記憶させ、暗証照合時には暗号化された暗証符号同士を、復号化することなしに暗証照合を行うことにより、暗証符号を第3者から保護するように構成したICカード暗証照合システム。

(2) 暗号入力装置における暗号化鍵生成手段は、暗号化鍵を生成するのに必要なデータが記憶されているルックアップテーブルメモリからなる特許請求の範囲第1項記載のICカード暗証照合システム。

3、発明の詳細な説明

産業上の利用分野

本発明は、主としてキャッシュカード，クレジットカードなどの電子的資金移動(EFT)取引に用いられるICカードの正当性を確認するための暗証符号照合システムに関するものである。

従来の技術

第3図は、従来のICカード暗証照合システム

における一構成例を示したものである。第３図において、３１０はＩＣカード所持者が暗証符号を入力する暗証符号入力手段３０１から得られる入力暗証符号を出力する暗証入力装置、３２０はカード発行時などに登録される登録暗証符号を記憶するメモリ手段３０２と、前記登録暗証符号と前記入力暗証符号との照合を行い照合結果を出力する暗証照合手段３０３から構成されるＩＣカードである。３３０は前記暗証入力装置３１０から得られる入力暗証符号を前記ＩＣカード３２０に書き込み、前記ＩＣカード３２０から前記登録暗証符号と前記入力暗証符号の照合結果を読み出すＩＣカード端末機である。

以上のように構成された従来のＩＣカード暗証照合システムについて、以下にその動作の説明を行う。

ＩＣカード所持者がＩＣカード３２０をＩＣカード端末機３３０に装着した後、暗証符号入力手段３０１から暗証符号を入力すると、入力された暗証符号は暗証入力装置３１０から入力暗証符号としてＩＣカード端末機３３０に入力され、ＩＣカード３２０内の暗証照合手段３０３の一入力に加えられる。一方、ＩＣカード３２０内のメモリ手段３０２に記憶された登録暗証符号は、前記暗証照合手段３０３の他の入力に加えられ、入力暗証符号との照合がとられる。ＩＣカード端末機３３０は暗証符号の照合結果をＩＣカード３２０から読み取り、カード所持者の本人確認を行う。

発明が解決しようとする問題点

このような従来のＩＣカード暗証照合システムでは、暗号化されていない暗証符号を用いて暗証照合を行うため、暗号化されていない暗証符号が暗証入力装置３１０からＩＣカード３２０まで伝送され、カード所有者以外の第３者に暗証符号が伝わる危険性があった。また、このような従来のシステムに用いられるＩＣカード３２０には、暗号化されていない暗証符号が記憶されるため、カード紛失時にはカード所有者以外に暗証符号が盗まれる可能性があった。現在のＩＣカードを用いた取引において、カード所持者の本人確認には、暗証符号の利用以外に方法が無く、暗証符号を第３者から保護することはＩＣカードのセキュリティ上、きわめて重要である。

本発明はかかる問題点に鑑みてなされたもので、簡易な構成で暗証符号を第３者から保護することのできるＩＣカード暗証照合システムを提供することを目的としている。

問題点を解決するための手段

本発明は上記問題点を解決するため、カード所持者が暗証符号を入力する暗証符号入力手段、前記暗証符号入力手段から得られる第１の入力暗証符号を用いて暗号化鍵を生成する暗号化鍵生成手段、および前記暗号化鍵を用いて前記第１の入力暗証符号を暗号化された第２の入力暗証符号に変換する暗証符号暗号化手段とを具備する暗証入力装置と、カード発行時などに登録される登録暗証符号を記憶するメモリ手段、および前記登録暗証符号と前記第２の入力暗証符号との照合を行い照合結果を出力する暗証照合手段とを具備するＩＣカードと、前記暗証入力装置から得られる第２の入力暗証符号を前記ＩＣカードに書き込み、前記ＩＣカードから前記登録暗証符号と前記第２の入力暗証符号の照合結果を読み出すＩＣカード端末機とを有し、前記登録暗証符号を、前記暗号化鍵と同一の暗号化鍵と前記暗証符号暗号化手段と同一の手続きを用いて暗号化し、前記メモリ手段にまえもって記憶させ、暗証照合時には暗号化された暗証符号同士を、復号化することなしに暗証照合を行うことにより、暗証符号をカード所有者以外の第３者から保護するように構成したものである。

作用

このように構成されたＩＣカード暗証照合システムにおいて、暗号化鍵生成手段は、暗証符号入力手段から得られる第１の入力暗証符号を用いて暗号化鍵を生成し、暗証符号暗号化手段は、前記暗号化鍵を用いて前記第１の入力暗証符号を暗号化して第２の入力暗証符号に変換し、暗証入力装置は、こうして暗号化された第２の入力暗証符号をＩＣカード端末機に対して出力する。

ＩＣカード端末機は、前記暗証入力装置から得られた第２の入力暗証符号をＩＣカード内に書き込み、ＩＣカードから出力される照合結果を待つ。

一方、メモリ手段は、カード発行時などに登録される登録暗証符号を記憶しておき、暗証照合手段は、前記登録暗証符号と前記第２の入力暗証符号との照合を行い、ＩＣカードは、このようにして照合結果をＩＣカード端末機に提供する。

このとき、前記登録暗証符号を、前記暗号化鍵と同一の暗号化鍵と前記暗証符号暗号化手段と同一の手続きを用いて暗号化し、前記メモリ手段にあえもって記憶させ、暗証照合時には暗号化された暗証符号同士を、復号化することなしに暗証照合することにより、暗証符号をカード所有者以外の第３者から保護することが可能となる。

実施例

以下、本発明の実施例を図面を参照しながら説明する。第１図は、本発明によるＩＣカード暗証照合システムの一実施例を示している。

第１図において、１２０はメモリ手段１０４と暗証照合手段１０５から構成されるＩＣカード、１３０はＩＣカード端末機で、これらは第３図の従来例の構成と同じものである。

１０１はＩＣカード所持者が暗証符号を入力する手段を提供する暗証符号入力手段、１０２は暗証符号入力手段１０１から得られる第１の入力暗証符号ＰＩＮ１から暗号化鍵ＫＥＹを生成する暗号化鍵生成手段、１０３は暗号化鍵生成手段102から得られる暗号化鍵ＫＥＹを用いて第１の入力暗証符号ＰＩＮ１を暗号化し第２の入力暗証符号ＰＩＮ２に変換する暗証符号暗号化手段である。

また、１１０は暗証符号入力手段１０１と暗号化鍵生成手段１０２と暗証符号暗号化手段１０３からなる暗証入力装置である。

以上のように構成されたＩＣカード暗証照合システムについて、以下にその動作の説明を行う。

ＩＣカード所有者がＩＣカード１２０をＩＣカード端末機１３０に装着した後、暗証符号入力手段１０１から暗証符号を入力すると、入力された暗証符号は第１の入力暗証符号ＰＩＮ１として暗号化鍵生成手段１０２と暗証符号暗号化手段103に加えられる。暗号化鍵生成手段１０２は、暗証符号入力手段１０１から得られる第１の入力暗証符号ＰＩＮ１を用いて暗号化鍵ＫＥＹを生成し、暗証符号暗号化手段１０３は、暗号化鍵生成手段１０２から得られる暗号化鍵ＫＥＹを用いて第１の入力暗証符号ＰＩＮ１を暗号化し、暗証入力装置１１０はこうして暗号化された第２の入力暗証符号ＰＩＮ２をＩＣカード端末機１３０に対して出力する。

ＩＣカード端末機１３０は、暗証入力装置110から得られる第２の入力暗証符号ＰＩＮ２をＩＣカード１２０に書き込み、ＩＣカード１２０から暗証符号の照合結果ＡＮＳが出力されるのを待つ。

一方、ＩＣカード１２０内のメモリ手段１０４に記憶されている登録暗証符号ＰＩＮ３は、暗証照合手段１０５によって読み出され、ＩＣカード端末機１３０から入力された第２の入力暗証符号ＰＩＮ２との暗証照合を行い、ＩＣカード１２０はこのようにして得られた照合結果ＡＮＳをＩＣカード端末機１３０に対して出力する。

ただし、本実施例における登録暗証符号PIN3は、暗号化鍵生成手段１０２で生成される暗号化鍵ＫＥＹと同一の暗号化鍵と暗証符号暗号化手段１０３で用いられる暗号化の手続きと同一の手続きにより、カード発行時などにあえもって暗号化され、ＩＣカード１２０内のメモリ手段１０４に記憶されている。

第２図は、本発明によるＩＣカード暗証照合システムに用いられる暗号化鍵生成手段の一実施例を示している。第２図ａは、ルックアップテーブルメモリＬＵＴにより、暗証符号ｎが暗号化KEYnに変換されるようすを模式的に表している。第２図ｂは、前記ルックアップテーブルメモリＬＵＴに記憶されている変換規則を示している。

第２図において、暗証符号入力手段１０１から入力される暗証符号ｎがルックアップテーブルメモリＬＵＴのアドレス入力に加えられると、前記ルックアップテーブルメモリＬＵＴのデータ出力から前記暗証符号ｎに対応した暗号化鍵ＫＥＹｎ

が出力される。

発明の効果

以上述べてきたように本発明によれば、簡易な構成で、暗証符号を第３者から保護することができ、ＩＣカードのセキュリティ上、きわめて有用なものとなる。

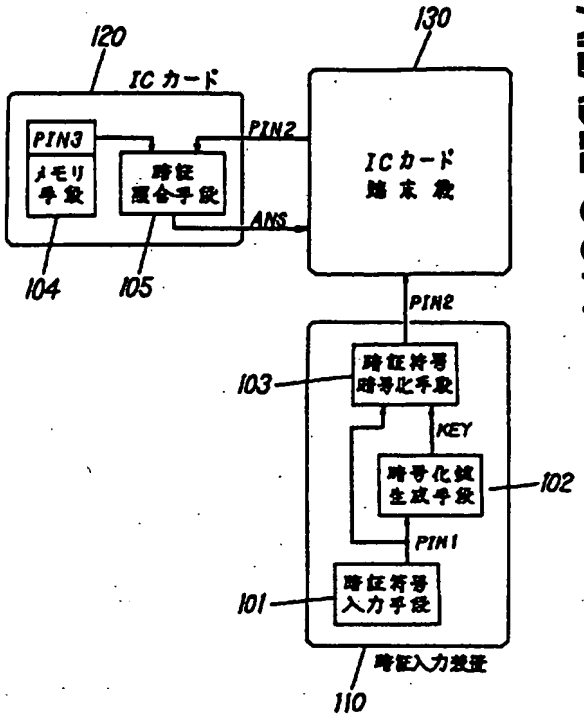
4、図面の簡単な説明

第１図は本発明によるＩＣカード暗証照合システムの一実施例の構成をブロック図で示す図、第２図は第１図に示した本発明の実施例に用いられた暗号化鍵生成手段の一実施例の構成を具体例で示す図、第３図は従来のＩＣカード暗証照合システムの一構成例をブロック図で示す図である。

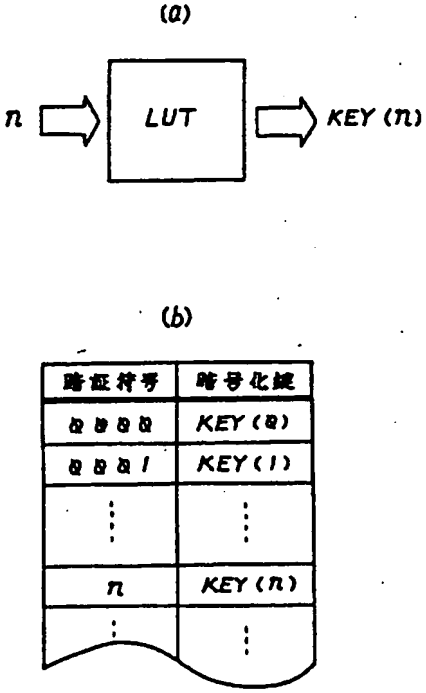
１０１……暗証符号入力手段、１０２……暗号化鍵生成手段、１０３……暗証符号暗号化手段、１０４……メモリ手段、１０５……暗証照合手段、１１０……暗証入力装置、１２０……ＩＣカード、１３０……ＩＣカード端末機。

代理人の氏名　弁理士　中　尾　敏　男　ほか１名

第１図



第２図



第３図